CLAIMS

What is claimed is:

1. A method for monitoring network packets within a distributed data processing system, the method comprising:

monitoring multiple sources of network packets within the distributed data processing system;

identifying a source of network packets as generating network packets having characteristics related to packet size that satisfy one or more predetermined conditions; and

alerting a system administrator to the identified source of network packets.

2. The method of claim 1 wherein a predetermined condition is a packet size less than a predetermined packet size threshold value.

3. The method of claim 1 wherein a predetermined condition is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size.

4. The method of claim 1 wherein a predetermined condition is a count of a number of packets satisfying one or more predetermined conditions that exceed a predetermined maximum count threshold value.

5. The method of claim 1 wherein a predetermined condition is a computed percentage value of a number of packets satisfying one or more predetermined conditions in comparison to a number of packets from the identified source of network packets.

6. The method of claim 1 further comprising:

in response to a request of the system administrator, halting execution of the identified source.

7. The method of claim 1 further comprising:

in response to a request of the system administrator, pausing execution of the identified source.

8. The method of claim 1 further comprising:

initiating a packet snooping session.

9. The method of claim 8 further comprising:

deploying distributed packet snoopers from a packet usage manager to monitor the multiple sources of network packets.

10. The method of claim 9 further comprising:

receiving packet filtering parameters at a distributed packet snooper;

matching packet filtering parameters against transmitted packets; and

returning packet usage events to the packet usage manager in response to a determination that a packet surpassed a limitation specified by the packet filtering parameters.

11. The method of claim 10 further comprising:

receiving a request for an action at a target resource within the distributed data processing system, wherein completion of the action depends upon operations of a set of resources along a logical route through the distributed data processing system, wherein the request for the action at the target resource is associated with a user or an application.

12. The method of claim 11 further comprising:

deriving one of the packet filtering parameters from an application or a user associated with the request for the action at the target resource.

13. The method of claim 11 further comprising:

selecting by the system administrator one of the packet filtering parameters by choosing among a plurality of active applications or users within the data processing system.

14. The method of claim 11 further comprising:

deriving a set of logical routes from a network topology mapping, wherein each logical route is a series of endpoints that comprise an endpoint-to-endpoint route for completing the requested action.

15. The method of claim 1 further comprising:

displaying the identified source of network packets to the system administrator in real time.

16. An apparatus for monitoring network packets within a distributed data processing system, the apparatus comprising:

means for monitoring multiple sources of network packets within the distributed data processing system;

means for identifying a source of network packets as generating network packets having characteristics related to packet size that satisfy one or more predetermined conditions; and

means for alerting a system administrator to the identified source of network packets.

17. The apparatus of claim 16 wherein a predetermined condition is a packet size less than a predetermined packet size threshold value.

18. The apparatus of claim 16 wherein a predetermined condition is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size.

19. The apparatus of claim 16 wherein a predetermined condition is a count of a number of packets satisfying one or more predetermined conditions that exceed a predetermined maximum count threshold value.

20. The apparatus of claim 16 wherein a predetermined condition is a computed percentage value of a number of packets satisfying one or more predetermined conditions in comparison to a number of packets from the identified source of network packets.

21. The apparatus of claim 16 further comprising:

means for halting execution of the identified source in response to a request of the system administrator.

22. The apparatus of claim 16 further comprising:

means for pausing execution of the identified source in response to a request of the system administrator.

23. The apparatus of claim 16 further comprising:

means for initiating a packet snooping session.

24. The apparatus of claim 23 further comprising:

means for deploying distributed packet snoopers from a packet usage manager to monitor the multiple sources of network packets.

25. The apparatus of claim 24 further comprising:

means for receiving packet filtering parameters at a distributed packet snooper;

means for matching packet filtering parameters against transmitted packets; and

means for returning packet usage events to the packet usage manager in response to a determination that a packet surpassed a limitation specified by the packet filtering parameters.

26. The apparatus of claim 25 further comprising:

means for receiving a request for an action at a target resource within the distributed data processing system, wherein completion of the action depends upon operations of a set of resources along a logical route through the distributed data processing system, wherein the request for the action at the target resource is associated with a user or an application.

27. The apparatus of claim 26 further comprising:

means for deriving one of the packet filtering parameters from an application or a user associated with the request for the action at the target resource.

28. The apparatus of claim 26 further comprising:

means for selecting by the system administrator one of the packet filtering parameters by choosing among a plurality of active applications or users within the data processing system.

29. The apparatus of claim 26 further comprising:

means for deriving a set of logical routes from a network topology mapping, wherein each logical route is a series of endpoints that comprise an endpoint-to-endpoint route for completing the requested action.

30. The apparatus of claim 16 further comprising:

means for displaying the identified source of network packets to the system administrator in real time.

31. A computer program product in a computer-readable medium for use within a distributed data processing system for monitoring network packets, the computer program product comprising:

instructions for monitoring multiple sources of network packets within the distributed data processing system;

instructions for identifying a source of network packets as generating network packets having characteristics related to packet size that satisfy one or more predetermined conditions; and

instructions for alerting a system administrator to the identified source of network packets.

32. The computer program product of claim 31 wherein a predetermined condition is a packet size less than a predetermined packet size threshold value.

33. The computer program product of claim 31 wherein a predetermined condition is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size.

34. The computer program product of claim 31 wherein a predetermined condition is a count of a number of packets satisfying one or more predetermined conditions that exceed a predetermined maximum count threshold value.

35. The computer program product of claim 31 wherein a predetermined condition is a computed percentage value of a number of packets satisfying one or more predetermined conditions in comparison to a number of packets from the identified source of network packets.

36. The computer program product of claim 31 further comprising:

instructions for halting execution of the identified source in response to a request of the system administrator.

37. The computer program product of claim 31 further comprising:

instructions for pausing execution of the identified source in response to a request of the system administrator.

38. The computer program product of claim 31 further comprising:

instructions for initiating a packet snooping session.

39. The computer program product of claim 38 further comprising:

instructions for deploying distributed packet snoopers from a packet usage manager to monitor the multiple sources of network packets.

40. The computer program product of claim 39 further comprising:

instructions for receiving packet filtering parameters at a distributed packet snooper;

instructions for matching packet filtering parameters against transmitted packets; and

instructions for returning packet usage events to the packet usage manager in response to a determination that a packet surpassed a limitation specified by the packet filtering parameters.

41. The computer program product of claim 40 further comprising:

instructions for receiving a request for an action at a target resource within the distributed data processing system, wherein completion of the action depends upon operations of a set of resources along a logical route through the distributed data processing system, wherein the request for the action at the target resource is associated with a user or an application.

42. The computer program product of claim 41 further comprising:

instructions for deriving one of the packet filtering parameters from an application or a user associated with the request for the action at the target resource.

43. The computer program product of claim 41 further comprising:

instructions for selecting by the system administrator one of the packet filtering parameters by choosing among a plurality of active applications or users within the data processing system.

44. The computer program product of claim 41 further comprising:

instructions for deriving a set of logical routes from a network topology mapping, wherein each logical route is a series of endpoints that comprise an endpoint-to-endpoint route for completing the requested action.

45. The computer program product of claim 41 further comprising:

instructions for displaying the identified source of network packets to the system administrator in real time.